الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد حمة لخضر
كلية العلوم الإسلامية

عنوان المحاضرة :

عالم الفيروسات virus

بقلم الأستاذ: ذويب العروسي

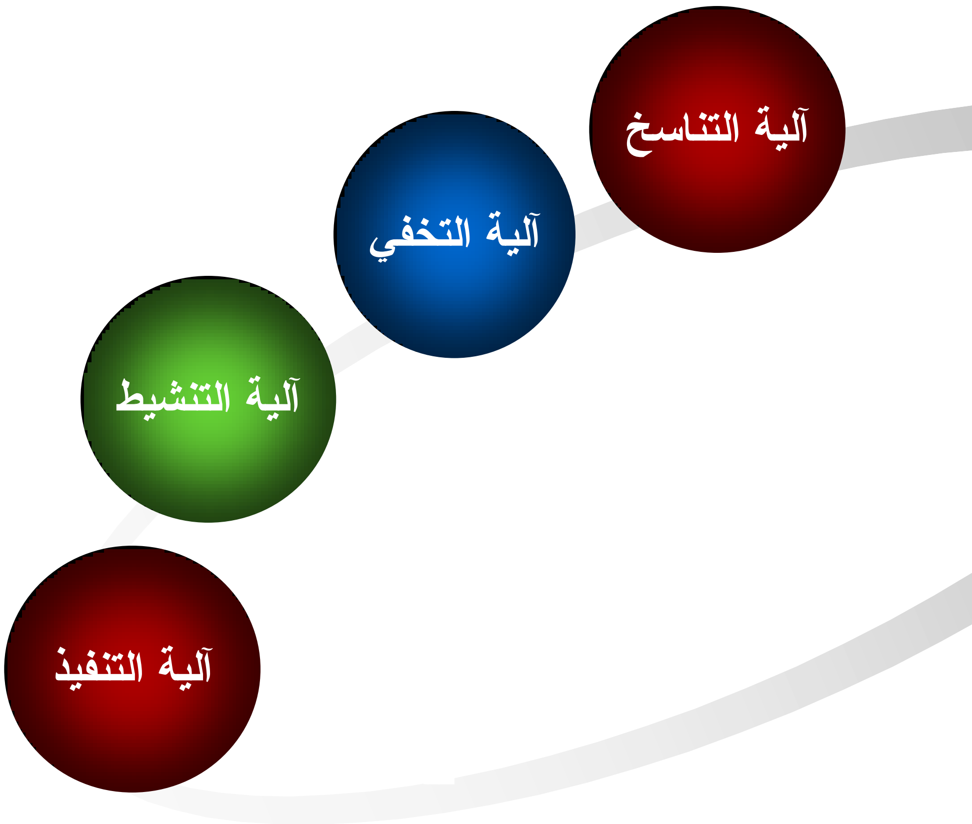
تعريف الفيروس

- فيروس الحاسوب هو برنامج خارجي صنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. اي ان فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

يتصف فيروس الحاسب بأنه :

1. برنامج قادر على التناسخ Replicationوالانتشار.
2. الفيروس يربط نفسه ببرنامج أخر يسمى الحاضن .host
3. يمكن أن تنتقل من حاسوب مصاب لآخر سليم.
4. لا يمكن أن تنشأ الفيروسات من ذاتها.

مكونات الفيروس



وهو الجزء الذي يسمح للفيروس أن ينسخ نفسه.

وهو الجزء الذي يخفي الفيروس عن الاكتشاف..

وهو الجزء الذي يسمح للفيروس بالانتشار قبل أن يعرف وجوده كاستخدام توقيت الساعة في الحاسوب كما في فيروس الذي ينشط (Michelangelo) في السادس من آذار من كل عام.

وهو الجزء الذي ينفذ الفيروس عندما يتم تنشيطه

اللغات التي يكتب بها الفيروس:

من أهم اللغات التي يكتب بها كود الفيروس هي لغة التجميع اسمبلي لسهولة الوصول لعتاد الحاسوب وهنا أيضاً اللغات الراقية مثل لغة سي ولغة سي ++ وفيجوال سي وفيجوال بيسك.

أسباب التسمية:

سمي الفيروس Virus بهذا الاسم لأنها تشبه تلك الكائنات المتطفلة في صفتين رئيسيتين:
اولا : فالفيروسات دائماً تتستر خلف ملف آخر، ولكنها تأخذ زمام السيطرة على البرنامج المصاب. بحيث أنه حين يتم تشغيل البرنامج المصاب، يتم تشغيل الفيروس أيضا ثانيا : تتواجد الفيروسات في مكان أساسي في الحاسب كالذاكره رام مثلا وتصيب اي ملف يشغل في أثناء وجودها بالذاكره مما يزيد عدد الملفات المصابه كلما طال وقت اكتشاف الفايروس تستخدم عادة لغة التجميع (الاسمبلي) لكتابة كود تنفيذ الفيروس

طرق الإنتقال:

أهم طرق الانتقال الآن هي الشبكة العنكبوتية الإنترنت تكون وسيلة سهلة لانتقال الفيروسات من جهاز لاخر ما لم تستخدم أنظمة الحماية مثل الجدران النارية وبرامج الحماية من الفيروسات ياتي ثانيا وسائط التخزين مثل ذواكر الفلاش والاقراص الضوئية والمرنة سابقا وياتي أيضا ضمن رسائل البريد الإلكتروني وأيضا تنتقل الفيروسات إلى نظامك عند استلامه ملفات اي كانت الملفات مخزنة على(اقراص مرنة أو اقراص مضغوطة أو اقراص)

أعراض الإصابة:

- تكرار رسائل الخطأ في أكثر من برنامج.
- ظهور رسالة تعذر الحفظ لعدم كفاية المساحة.
- تكرار اختفاء بعض الملفات التنفيذية.
- حدوث بطء شديد في إقلاع[نظام التشغيل]أو تنفيذ بعض التطبيقات. رفض بعض التطبيقات للتنفيذ.



أنواع الفيروسات:



الديدان worm :

تصيب الديدان الكمبيوترات الموصلة بالشبكة بشكل اوتوماتيكي و من غير تدخل الانسان و هذا الامر يجعلها تنتشر بشكل اوسع و اسرع عن الفيروسات . الفرق بينهم هو ان الديدان لا تقوم بحذف او تغيير الملفات بل تقوم بتهليك موارد الجهاز و استخدام الذاكرة بشكل فظيع مما يؤدي الى بطء ملحوظ جدا للجهاز



أنواع الفيروسات:



الفيروس :

الفيروس: يمكن القول بأنه برنامج تنفيذي يعمل بشكل منفصل ويهدف إلى أحداث خلل في نظام الحاسوب وتترواح خطورتة حسب مهمته فمنه الخطير ومنه الخفيف وكلاهما خبيث.وينتقل بواسطة نسخ الملفات من جهاز به ملفات مصابة إلى جهاز اخر عن طريق الاقراص المدمجة سي دي وذواكر الفلاش.

أنواع الفيروسات:



حصان طروادة: Trojan Horse

سمي هذا الفيروس بحصان طروادة لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله واستطاعوا اقتحام مدينة طروادة والتغلب على جيشها وهكذا تكون آلية عمل هذا الفيروس حيث يكون مرفقا مع أحد البرامج أي يكون جزء من برنامج مادون إن يعلم المستخدم.



أنواع الفيروسات:



حصان طروادة: Trojan Horse

برنامج يغري المستخدم باهميته او بشكله او باسمه ان كان جذاباً، و في الواقع هو برنامج يقوم بفتح باب خلفي بمجرد تشغيله ، و من خلال هذا الباب الخلفي يقوم المخترق باختراق الجهاز و بامكانه التحكم بالجهاز بشكل كبير.

امثلة على بعض الفيروسات

:My doom

قدر الخبراء الحواسيب المتضررة من هذه الدودة بحوالي ربع مليون حاسوب خلال يوم واحد والذي كان في كانون الثاني 2004

:Melissa

في ربيع 1999 شخص يُدعى ديفيد سميث صنع فيروس يُصيب ميكروسوفت وورد ماكرو بحيث ينتشر عبر رسائل الايميل وسمّاه ميليسًا يقوم الفيروس باغراء المستخدمين للايميل عن طريق ارسال ملف في رسالة ايميل ومكتوب فيها

" Here is that document you asked for, don't show it to anybody else."

وبمجرد ان تقوم بفتح الملف يتم تنشيط الفيروس

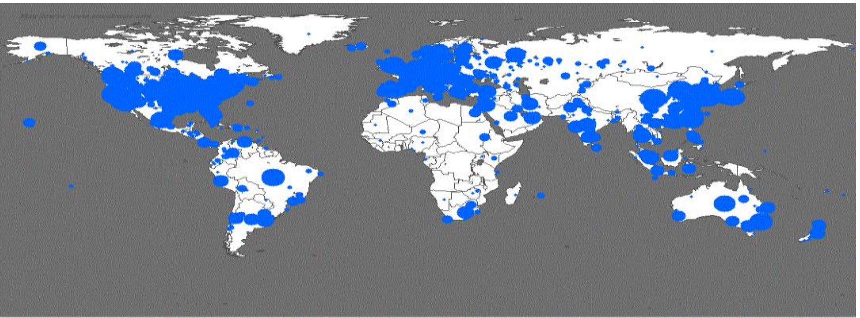
وينسخ نفسه ويرسل نفسه الى اهم 50 شخص لديك عبر البريد الالكتروني

- انتشر الفيروس بسرعة كبيرة بعد ان اطلقه سميث واصبحت الحكومة الفيدرالية في امريكا مهتمة بما يقوم به سميث هذا لان انتشار الفيروس اصبح كبيرا لدرجة انه منع برامج الايميلات من الاستمرار في العمل وبعد الكثير من المحاولات الطويلة تم القبض على سميث وتم سجنه 20 شهر ومنعته من استخدام شبكات الكمبيوتر بدون اذن من المحكمة صحيح ان الفيروس لم يصيب الانترنت بشلل حقيقي الا انه يعتبر من اول الفيروسات التي لفتت الانتباه الى اهمية مثل هذه البرامج



❖ SQL slammer:

في اواخر يناير عام 2003 ظهر نوع جديد من الفيروسات التي تصيب الخوادم وينتشر عبر الانترنت وكانت العديد الشبكات غير مستعدة لمثل هذا الهجوم فنتج عن ذلك انهيار الكثير من انظمة الخوادم المهمة ، فقد انهار امامه النظام للبنك الامريكي لخدمات ATM ورحلات طيران شركة كونتينتال وقامت بالغاء الكثير من الرحلات وتعطل الحجز الالكتروني للتذاكر وتسبب الفيروس في هذا اليوم بخسائر تقدر بمليار دولار ولم تستطيع البرامج المضادة للفيروسات ان تلاحق هذا الفيروس وقد احتاج هذا الفيروس الى 15 دقيقة فقط لكي يُصيب نصف عدد الخوادم الداعمة للانترنت



❖ فيروس leap A/ Oompa A :

في اعلانات ابل كانت تفتخر بان نظام التشغيل لديها منيع ضد الفيروسات و هذا الكلام يمكن ان يعتبر صحيح بشكل كبير حيث ان ابل تغلق على مكونات اجهزتها وطريق برمجة انظمة التحكم لديها بشكل كبير ولكن هذا كله توقف عام 2006 امام هذا الفيروس حيث يستخدم الشات ولحظة ارسال الرسالة حتى ينتشر عبر نقاط ضعف كمبيوتر الماك ولكن المُطمئن ان هذا الفيروس ليس خطير بدرجة كبيرة ولكنه اوضح ان حتى الماك ليس حصين ضد الفيروسات



- فيروس العاصفة (storm worm):

ينتشر عبر الايميل ويمكن ان يغير عنوان الميل باشكال مختلفة فقد ظهر في 2008 في الصين بعنوان كارثة مميتة جديدة في الصين "a new deadly catastrophe in china" يحتوي الايميل على لينك فيديو ما ان تضغط على اللينك حتى يتم تفعيل الفيروس وتحميله لذلك يجب ان يكون مضاد الفيروسات الخاص بك حديث الاصدار



- فيروس xcopy والذي يصيب الـ Partion القسم للقرص الصلب ويجعله لايفتح مباشرة وذلك بزرع ملف autorun وحينما تحاول فتح القسم يعطيك قائمة فتح باستخدام ولا تستطيع الدخول إلى القسم الذي تريده إلا بطرق ملتوية مثل (استكشاف وتشغيل للمحترفين فقط ويقوم أيضا بجعل الفلوبي دسك القرص المرن يصيح باستمرار مطالبا بإدخال قرص مرن للكمبيوتر



Stuxnet – 2010:

واحد من أكثر الفيروسات التى تسبب فى إحداث أضرار ، فلم تكتف الدودة بمهاجمة أجهزة المستخدمين العاديين ، بل قامت دودة Stuxnet بأعمال تجسس على الأنظمة الصناعية التى تعمل على نظام ويندوز وإعادة برمجتها ، وخاصة نظام SCADA الذى يستخدم فى مجالات تنظيم حركة السير، وخطوط الأنابيب وإدارة المفاعلات النوويّة ، وضربت دودة Stuxnet عدة منشآت صناعية هامة كمفاعل بوشهر النووى بإيران فضلا عن 15 مؤسسة صناعية أخرى ، الجدير بالذكر أن إيران تحملت 60% من إجمالى الخسائر التى سببها Stuxnet مما يبين أن الهدف من وراء Stuxnet كانت أهداف سياسية تقف وراءها قوى دولية .

طرق الحماية من الفيروسات:

1) تنصيب البرامج المضادة للفيروسات.
2) نكتفي بتنصيب البرامج الموثوق منها فقط.
3) التحديث المستمر لنظام التشغيل.
4) تركيب الجدار الناري.
5) عدم فتح الملفات المرفقة مع البريد الالكتروني إلا إذا كان المصدر موثوقا.
6) تنصيب البرامج المكملة لمضادات الفيروسات.
7) عدم دخول المواقع التي يحذرنا منها متصفح الانترنت.

الخلاصة : لماذا يعمل الناس فيروسات الحاسوب ؟

- فيروس الحاسوب يتم برمجته من قبل المبرمجين أو الشركات ويتم صنعه بشكل متعمد ويتم تصميمه بشكل متقن. يعمل المبرمجون على برمجة الفيروسات وذلك لاهداف عديدة تتنوع من اقتصادية وسياسية وتجارية وعسكرية. فبعض المبرمجين الهواة يعتبرون أن عمل الفيروس نوع من الفن والهواية التي يمارسونها. ومن أهم الأهداف لعمل فيروس الحاسوب هو الهدف التجاري. ذلك عن طريق عمل وصنع الفيروسات من أجل بيع برامج مضادات الفيروسات لانة بعمل الفيروس يصبح المستخدمون بحاجة إلى برامج مضادة للفيروسات ويضطرون للشراء. يذكر أن المبرمج الذي يعمل الفيروس يعتبر حسب القانون مجرما وصناعة الفيروس جريمة يحاسب عليها حسب قانون الدولة الموجود بها.

- معظم شركات مضادات الفيروسات تقوم بصناعة الفيروسات من قبل المبرمجين وتقوم بعمل مضادات لها وذلك لتسويق منتجاتها وبرامجها لدى مستخدمي الكمبيوتر. اما الاهداف العسكرية فهي محاولة الدخول لأنظمة الطرف الاخر لكشف اسرار واخذ بيانات عن طريق برامج التجسس. الاهداف الإجرامية فأهمها سرقة بيانات وارقام حسابات أو ارقام بطاقات الائتمان وكلمات السر لمحاولة الدخول

شكرا لكم على حسن استماعكم

Larouci.douib.info@gmail.com